ABSTRACT OF THE DISCLOSURE

An arithmetic apparatus for performing a long

product-sum operation includes an integer unit

arithmetic circuit, a finite field $GF(2^m)$ based unit

5   arithmetic circuit logically adjacent to the integer

unit arithmetic circuit, a selector for selecting the

integer unit arithmetic circuit or the finite field

$GF(2^m)$ based unit arithmetic circuit, and an adder

circuit which has a buffer for storing interim result

10   data, adds the interim result data to the result data

obtained by one of the integer unit arithmetic circuit

and the finite field $GF(2^m)$ based unit arithmetic

circuit which is selected by the selector, propagates a

carry in an integer unit arithmetic operation, and

15   propagates no carry in a finite field $GF(2^m)$ based unit

arithmetic operation.